

Wellworth Financial Services Pvt. Ltd.

Document Control Page

Document Name	PMLA Compliance Policy
Applicability	NBFC

Authorization	Document Owner	Last Reviewed On
Name	Wellworth Financial Services Pvt Ltd	21.06.2024
Signature	Sd/-	

All queries, suggestions and changes required may be emailed to nbfc@wellworthgroup.co (Principal Officer).

The information contained in this document is CONFIDENTIAL and may be legally PRIVILEGED. Any disclosure, copying, distribution, dissemination, forwarding, printing or any action taken in reliance on it or utilizing the same for any purpose other than what it is intended for, without consulting the Wellworth Financial Services Ltd is prohibited and may be unlawful

Background

The Prevention of Money Laundering Act, 2002 ("PMLA") was brought into force with effect from 1st July 2005. Necessary Notifications / Rules under the said Act were published in the Gazette of India on July 01, 2005 by the Department of Revenue, Ministry of Finance, Government of India.

As per the provisions of the PMLA, every banking company, financial institution (which includes chit fund company, a co-operative bank, a housing finance institution and a non-banking financial company) and intermediary (which includes a stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under Section 12 of the SEBI Act, shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules under the PMLA. Such transactions include:

- i. All cash transactions of the value of more than Rs. 10 lakh or its equivalent in foreign currency.
- ii. All series of cash transactions integrally connected to each other which have been valued below Rs. 10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency
- iii. All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account such as demat account, security account maintained by the registered intermediary.

For the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' shall also be considered. In case there is a variance in CDD/AML standards prescribed by the RBI and the regulators of the host country, branches/overseas subsidiaries of intermediaries are required to adopt the more stringent requirements of the two.

This Policy only supplements the existing RBI/ FIU guidelines relating to KYC/AML and any subsequent guidelines from the date of the Policy on KYC/AML will be implemented immediately, with subsequent ratification by the Board. Extant regulations will at any point in time override this Policy.

Policy

Prevention of Money Laundering Act, 2002

1. Policy Guidelines on 'Know Your Customer' norms And Anti-Money Laundering measures:

In terms of the guidelines issued by the Reserve Bank of India (RBI) on Know Your Customer (KYC) standards and Anti Money Laundering (AML) measures, NBFCs are required to put in place a comprehensive policy frame work covering KYC Standards and AML Measures.

For the purpose of this policy, the Wellworth Financial Services Pvt Ltd shall be referred as **the RE**.

Accordingly, this policy document is prepared in line with the RBI guidelines regarding customer identification procedures, customer profiling based on the risk perception and monitoring of transactions on an ongoing basis. The objective of this policy document is to prevent the RE from being used, intentionally or unintentionally, by criminal elements for money laundering activities and for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

2. Definition of Money Laundering

Section 3 of the Prevention of Money Laundering [PML] Act 2002 has defined the “offence of money laundering” as under:

“Whoever directly or indirectly attempts to indulge or knowingly assists or knowingly is party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property are guilty of offence of money laundering”.

Money launders may use the system for clearing ‘money’ earned through criminal activities with the objective of hiding/disguising its source. The process of money laundering involves creating a web of financial transactions so as to hide the origin and true nature of these funds. Money launders also disguise the true source of funds by investing the funds earned out of terrorist / criminal activities through third party accounts

3. Obligations under Prevention of Money Laundering [PML] act 2002

Section 12 of PML Act 2002 places certain obligations on every banking company, financial institution and intermediary which include:

- Maintaining a record of prescribed transactions
- Furnishing information of prescribed transactions to the specified authority
- Verifying and maintaining records of the identity of its clients
- Adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF
- Develop staff members’ awareness and vigilance to guard against ML and TF

4. Policy Objectives

- a. To prevent criminal elements from using the RE's system for money laundering activities.
- b. To enable the RE to know / understand its customers and their financial dealings better, which in turn would help the RE to manage risks prudently.
- c. To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
- d. To comply with applicable laws and regulatory guidelines related to anti - money laundering.
- e. To take necessary steps to ensure that the concerned staff are adequately trained in KYC/AML procedures.

5. Customer Due diligence:

The RE shall have a system in place for acceptance of new client. The staff of the RE shall ensure the following at the time of acceptance of new client:

1. The Application forms for opening an account are issued only when the prospective client provides the valid reference & introducer for his account.
2. All accounts are opened only when the prospective client is present in person before the company official. All franchisee / branch are also instructed to open only those account for which valid reference and introducer is available and client is present in person before the sub broker.
3. The RE collects the details of location (permanent address, correspondence address and registered office address), occupation details, nature of business activities, financial details etc. before new clients is registered.
4. The company shall collect the various mandatory documents as required by law, including the proof of identity of the client. The company should check the reliability of the document by reviewing / checking the same from independent source like verifying the PAN from the income tax website, etc.
5. The company has a procedure to determine whether existing / potential client are not Politically Exposed Person (PEP) and in case of any person found to be a PEP entity then approval of senior management is necessary and systems to verify the source of funds of clients.
6. Check that the identity of the clients does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide
7. The company has a system in place to ensure that accounts are not opened in the name of anyone whose name appears in the UN or other specified list and the scan of all existing accounts has been carried out and the same is to be regularly reviewed.

8. The company periodically reviews the trading volumes of the clients and their financial strength in terms of annual income, net worth etc.
9. The company also monitors the financial transactions with clients for pay in payout of funds and securities.
10. The company has the policy not to deal in cash with any of the clients, all transactions, receipt or payment, are carried out only through account payee cheque and digital payment only.
11. The company transacts only in Indian Rupees and no other currencies are being used for trades with clients.
12. All funds are released to the client by account payee cheques and with details of the bank account of the client written on the cheque so as to restrict the client to deposit cheques in only those bank accounts for which details are provided to us. Majority of our payout goes via RTGS and NEFT only.
13. The CDD measures comprise the following:
 - a) Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement
 - b) Verify the client's identity using reliable, independent source documents, data or information
 - c) Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted
 - i. For clients other than individuals or trusts: Where the client is a person other than an individual or trust, viz., company, partnership or unincorporated association/body of individuals, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:
 - aa) The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

- bb) In cases where there exists doubt under clause (aa) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.
- cc) Where no natural person is identified under clauses (aa) or (bb) above, the identity of the relevant natural person who holds the position of senior managing official.
- ii. For client which is a trust: Where the client is a trust, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
- iii. Exemption in case of listed companies: Where the client or the owner of the controlling interest is a company listed on a stock exchange or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
- iv. Applicability for foreign investors: Intermediaries dealing with foreign investors' may be guided by the clarifications issued vide SEBI circulars CIR/MIRSD/11/2012 dated September 5, 2012 and CIR/ MIRSD/ 07/ 2013 dated September 12, 2013, for the purpose of identification of beneficial ownership of the client.
- v. The Stock Exchanges and Depositories shall monitor the compliance of the aforementioned provision on identification of beneficial ownership through half-yearly internal audits. In case of mutual funds, compliance of the same shall be monitored by the Boards of the Asset Management Companies and the Trustees and in case of other intermediaries, by their Board of Directors
- d) Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c).
- e) Understand the ownership and control structure of the client.
- f) Conduct ongoing due diligence and scrutiny, i.e. Perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, considering, where necessary, the client's source of funds; and
- g) Registered intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

6. Customer Acceptance Procedure

- No account shall be opened in anonymous or fictitious/benami name.
- No account shall be opened where the RE is unable to apply appropriate CDD measures, either due to non-cooperation of the customer or non-reliability of the documents/information furnished by the customer. The RE shall consider filing an STR, if necessary, when it is unable to comply with the relevant CDD measures in relation to the customer.
- No transaction or account-based relationship shall be undertaken without following the CDD procedure.
- The RE shall obtain the mandatory information to be sought for KYC purpose while opening client account and during the periodic updation as specified by the RBI from time to time.
- Additional information, where such information requirement has not been specified in this policy, shall be obtained with the explicit consent of the customer.
- The RE shall apply the CDD procedure at the unique customer identification code level. Thus, if an existing KYC compliant customer of the RE desires to open another account with the same RE, there shall be no need for a fresh CDD exercise.
- CDD Procedure shall be followed for all the joint account holders, while opening a joint account.
- The RE shall establish suitable system to ensure that the identity of the customer does not match with any person or entity, whose name appears in the sanctions lists issued from time to time.
- Where Permanent Account Number (PAN) is obtained, the same shall be verified from the verification facility of the issuing authority.
- Where an equivalent e-document is obtained from the customer, RE shall verify the digital signature as per the provisions of the Information Technology Act, 2000.
- Where Goods and Services Tax (GST) details are available, the GST number shall be verified from the search/verification facility of the issuing authority.
- Customer Acceptance Policy shall not result in denial of banking/financial facility to members of the general public, especially those, who are financially or socially disadvantaged.
- Where the RE forms a suspicion of money laundering or terrorist financing, and it reasonably believes that performing the CDD process will tip-off the customer, it shall not pursue the CDD process, and instead file an STR with FIU-IND.
- The RE will use RBI caution advices in determining the customer acceptance framework.

- **Clients of special category (CSC) include the following:**
 - Non-resident clients
 - High net-worth clients,
 - Trust, Charities, Non-Governmental Organizations (NGOs), organizations receiving donations.
 - Companies having close family shareholdings or beneficial ownership.
 - Politically Exposed Persons (PEP)
 - Companies offering foreign exchange offerings.
 - Clients in high risk countries where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, countries active in narcotics production, countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, countries against which government sanctions are applied, countries reputed any of the following - Havens/ sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.
 - Non face to face clients
 - Clients with dubious reputation as per public information available etc.

Risk Management

- The RE shall categorize its customers into 'High Risk / Medium Risk / Low Risk' according to risk perceived based on its experience and review it from time to time.
- Risk categorization of customers shall be undertaken on the basis of various factors, such as a customer's identity, social/financial status, nature of business activity, and information about the customer's business and their location, geographical risk covering customers as well as transactions, type of products/services offered, delivery channel used for delivery of products/services, types of transaction undertaken - cash, cheque/monetary instruments, wire transfers, forex transactions, etc.
- The RE may at its discretion identify additional factors that it may wish to utilize for customer acceptance based on risk profile determined by the RE.
 - i. The risk categorisation of a customer and the specific reasons for such categorisation shall be kept confidential and shall not be revealed to the customer to avoid tipping off the customer. Customers who may pose a particular risk to the Company and Money Laundering Deterrence Programme and the Company's reputation, and who should normally be treated as high risk and subject to enhanced Customer Due Diligence, include, but are not limited to the following:-

Members of the Company must not establish accounts or relationships involving unregulated money service businesses or unregulated businesses involved in aiming/gambling activities.

- Offshore Trusts, Special purpose Vehicles, International Business Companies which are established in locations with strict bank secrecy or confidentiality rules, or other legislation that may impede the application of prudent money laundering controls.

- Private companies or public companies not subject to regulatory disclosure requirements that are constituted in full or in part by bearer shares.
- Customers with complex account relationships – e.g. multiple accounts in one, customers with high value and/ or high frequency transactional behaviour.
- No account should be opened in anonymous or fictitious/benami name(s) i.e. to say the anonymous or fictitious/benami customers shall not be accepted.
- No account should be allowed to do further transactions if any judgement has been issued by SEBI or FIU regarding any order against them and thus will effectively and expeditiously implement the order.
- No account should be opened if appropriate due diligence measures cannot be applied to a customer for want of verification documents on account of non co-operation of the customer or non-reliability of the data/information furnished of the Company.

a. Non Face to Face Businesses

Members of the Company should apply Customer Due Diligence procedures which ensure that the process is equally as effective for non face to face customers as for face to face customers. Financial services and products are now frequently provided to non face to face customers via postal, telephone and electronic facilities including the Internet. Customer identification procedures in these circumstances should include appropriate measure to mitigate the risks posed by non face to face business. Ongoing due diligence and scrutiny of transactions and trading account should be conducted.

b. Correspondent Accounts

- The Company is not permitted to open or maintain “payable through accounts”, (being correspondent accounts that are used directly to transact business on their own behalf) without the written and ongoing annual approval of the Head of Compliance.

Customer Identification Procedure

- The RE shall undertake identification of customers in the following cases:
 - a. Commencement of an account-based relationship with the customer.
 - b. Carrying out any international money transfer operations for a person who is not an account holder of the RE.
 - c. When there is a doubt about the authenticity or adequacy of the customer identification data it has obtained.
 - d. Selling third party products as agents, selling their own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than rupees fifty thousand.
 - e. Carrying out transactions for a non-account-based customer, that is a walk-in customer, where the amount involved is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.

- f. When the RE has reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of rupees fifty thousand.
- g. The RE shall ensure that introduction is not to be sought while opening accounts.

- **Reliance on third party for verification of client identity**

The RE may rely on customer due diligence done by a third party, subject to the following conditions:

- a. Records or the information of the customer due diligence carried out by the third party is obtained immediately from the third party or from the Central KYC Records Registry.
- b. Adequate steps are taken by REs to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements shall be made available from the third party upon request without delay.
- c. The third party is regulated, supervised or monitored for, and has measures in place for, compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the PML Act.
- d. The third party shall not be based in a country or jurisdiction assessed as high risk.
- e. The ultimate responsibility for customer due diligence and undertaking enhanced due diligence measures, as applicable, will be with the RE.

- While undertaking customer identification, the decision-making functions of determining compliance with KYC shall not be outsourced.
- The RE shall be adequately satisfied with the information furnished by each new customer with respect to identity of the customer and the purpose of the intended nature of relationship with the RE.
- The RE shall ensure that its customer is not a fictitious person by verifying the identity of the customer through documentation and shall also carry out necessary checks, so as to confirm that the identity of the customer on the basis of the documents obtained does not match with any person with known criminal background or with banned entities, such as individual terrorists or terrorist organizations.
- The RE shall obtain self-attested documents from the customers containing details of proof of their identity and address as per list of officially valid documents issued by the RBI and as amended from time to time.
- In addition to verification through valid documents, the RE may also call for suitable introduction by a person known to the RE.

Identification of Beneficial Owner

For opening an account of a Legal Person who is not a natural person, the beneficial owner(s) shall be identified and all reasonable steps as per the PML Rules to verify his/her identity shall be undertaken keeping in view the following:

- (a) Where the customer or the owner of the controlling interest is (i) an entity listed on a stock exchange in India, or (ii) it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions, or (iii) it is a subsidiary of such listed entities; it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.
- (b) In cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases, satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature of the trust or other arrangements in place shall be obtained.

CDD measures in case of certain categories of non-individual customers

The CDD measures pertaining to following categories of non-individual customers have been amended to include certain additional information / document requirements:

- a) Companies - (i) the names of the relevant persons holding senior management position; and (ii) the registered office and the principal place of its business, if it is different.
- b) Partnership firms - (i) the names of all the partners; and (ii) address of the registered office, and the principal place of its business, if it is different.

Reliable and independent sources of identification to be made

The CDD, at the time of commencement of an account-based relationship or while carrying out occasional transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or any international money transfer operations, shall include: (a) Identification of the customer, verification of their identity using reliable and independent sources of identification, obtaining information on the purpose and intended nature of the business relationship, where applicable;

On-going Due Diligence

- The RE shall undertake on-going due diligence of customers to ensure that their transactions are consistent with their knowledge about the customers, customers' business and risk profile and the source of funds/wealth. The extent of monitoring shall be aligned with the risk category of the customer.
- Without prejudice to the generality of factors that call for close monitoring following types of transactions shall necessarily be monitored:
 - (a) Large and complex transactions including RTGS transactions, and those with unusual patterns, inconsistent with the normal and expected activity of the customer, which have no apparent economic rationale or legitimate purpose.
 - (b) Transactions which exceed the thresholds prescribed for specific categories of accounts.
 - (c) High account turnover inconsistent with the size of the balance maintained.
 - (d) Deposit of third-party cheques, drafts, etc. in the existing and newly opened accounts followed by cash withdrawals for large amounts.

For ongoing due diligence, the RE may consider adopting appropriate innovations including artificial intelligence and machine learning (AI & ML) technologies to support effective monitoring.

- The extent of monitoring shall be aligned with the risk category of the customer. Example: High risk accounts have to be subjected to more intensified monitoring.
 - (a) A system of periodic review of risk categorisation of accounts, with such periodicity being at least once in six months, and the need for applying enhanced due diligence measures shall be put in place.
 - (b) The transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies shall be closely monitored.

Periodic Updation of KYC

Periodic updation shall be carried out at least once every two years for high risk customers, once every eight years for medium risk customers and once every ten years for low risk customers.

The RE shall follow guidelines issued by the RBI for periodic updation of KYC.

Enhanced Due Diligence

(a) Non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

- The RE shall not on-board non-face-to-face customers.

(b) Accounts of Politically Exposed Persons:

- “Politically Exposed Persons” (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials.
- Generally, the RE would not open accounts of PEP. Decision to deal with such persons as a customer shall be taken up at a senior management level and shall be subjected to enhanced monitoring.
- The RE shall verify the current address through positive confirmation before allowing operations in the account, PAN shall be obtained from the customer and shall be verified, customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP, etc.

Information obtained from Customers

All the information collected from the customers by the RE shall be kept confidential and all such information shall be treated as per the agreement/terms and conditions signed by the customers.

7. Appointment of Principal Officer

The RE shall appoint a senior management officer to be designated as Principal Officer (PO) who shall be independent and report directly to the senior management or to the Board of Directors. The PO shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations. The name, designation and address of the Principal Officer shall be communicated to the FIU-IND.

8. Appointment of Designated Director

The company shall appoint a Designated Director, as required under the Rule 2 (ba) of PML. The Designated Director shall be responsible to discharge the legal obligations to report suspicious transactions to the authorities. The Designated Director will act as a central reference point to ensure overall compliance in facilitating onward reporting of suspicious transactions and assessment of potentially suspicious transactions. In case of any change in the Designated Director, the information regarding the same would be immediately be informed to FIU.

9. Maintenance of transactions of records

The RE shall maintain proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PML Rules, 2005), as mentioned below:

- (i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
- (ii) Series of all cash transactions individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs or its equivalent in foreign currency. It is clarified that for determining 'integrally connected transactions' 'all accounts of the same customer' should be taken into account.
- (iii) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place facilitating the transactions;
- (iv) All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account such as demat accounts..

Note: For recording all the suspicious transactions "transactions integrally connected", "transactions remotely connected or related" should also be considered in records.

10. Information to be preserved

The RE shall maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as to permit reconstruction of individual transaction, including the following information:

- The nature of the transactions.
- The amount of the transaction and the currency in which it was denominated.
- The date on which the transaction was conducted.
- The parties to the transaction.
- The origin of the transaction.

11. Records Maintenance:

- All necessary records on transactions, both domestic and international, should be maintained at least for the minimum period of 5 years from date of transaction between the RE and the client as prescribed in PMLA, 2002 and other legislations, regulations or exchange byelaws or circulars.
- The RE shall maintain records pertaining to the identification of the customers and their address obtained while opening the account and during the course of business relationship for at least 5 years after the business relationship is ended. The identification of records and transaction data should be made available to the competent authorities upon request.
- In situation where the records relate to on-going investigations or transactions, which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that case has been closed.
- The RE shall record and maintain and preserve the information regarding the transaction as provided in Rule 3 of the PML rules and the information of the same should be maintained for a period of 5 years or until the trail for the trade.
- The RE shall pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level shall be properly recorded. Such records and related documents shall be made available to help auditors to scrutinize the transactions and also to Reserve Bank/other relevant authorities. These records shall be preserved for 5 years.

12. Monitoring of transactions

- (a) Ongoing monitoring is an essential element of effective KYC/AML procedures. The RE shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations.
- (b) Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions shall, as far as possible be examined, and written findings together with all documents be retained and made available to Reserve Bank/other relevant authorities, on request.
- (c) The RE shall apply enhanced due diligence measures on high risk customers. In view of the risks involved in cash intensive businesses, accounts of bullion dealers(including sub-dealers) and jewelers should also be categorized by NBFCs as 'high risk' requiring enhanced due diligence.
- (c) The RE shall periodically review risk categorization of client accounts and the need for applying enhanced due diligence measures.

13. Procedure and manner of maintaining information:

- The company shall maintain information in respect of above transactions with its client in hard and soft copies and in accordance with the procedure and the Reserve Bank of India or the Securities and Exchange Board of India may specify manner as, as the case may be, from time to time.
- The company shall maintain such information in form specified above and at such intervals as may be specified by the Reserve Bank of India from time to time.
- The company to observe the procedure and the manner of maintaining information as specified by the Reserve Bank of India.

14. Reporting of Transactions:

- The company shall have a system of monitoring the transactions for which the principal officer will be required to review the transactions and generate alerts from the system for further investigation.
- The company should carry out due diligence and scrutiny of transactions to ensure that the transactions being conducted are consistent with the business and risk profile of the client and the information are periodically updated with the data / information of the clients.
- The person responsible for the department shall immediately notify to the principal officers or any other designated officer within the intermediary giving details of the alerts and the nature of suspicious activity. The principal officer would further investigate the transactions and call for further information to assess the genuinity of the transaction. If felt suspicious the principal officer would inform immediately the Financial Intelligence Unit (FIU) giving details of the transaction in the Suspicious Transaction Report (STR).

- The proper documents and supporting for the transaction should be maintained with the intermediary and forward the details as may be called by the regulators.
- The company shall have system of keeping a check on trading volume of client is in proportion to his financial details as disclosed in the KYC.

14. List of designated individuals/ Entities

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at <http://www.un.org/sc/committees/1267/consolist.shtml>. Registered intermediaries are directed to ensure that accounts are not opened in the name of anyone whose name appears in said list. Registered intermediaries shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to SEBI and FIU-IND.

15. Action On Reported Suspicious Transactions & Cash Transactions

- a. All reported suspicious transactions of any customer(s) with suspicious identity should be reviewed by the Principal Officer thoroughly. After thorough verification & confirmation of transactions which are suspicious in nature, the same should be immediately (not later than 7 days) reported to FIU, Ministry of Finance, New Delhi in writing

16. Reporting to Financial Intelligence Unit - India (FIU-IND):

The Principal Officer of the RE shall act as a central reference point in facilitating onward reporting of transactions to FIU-IND and for playing an active role in the identification and assessment of potentially suspicious transactions.

The Principal Officer of the RE shall submit Cash Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) as prescribed under Rule 3, notified under the PMLA to:

**Director, FIU-IND,
Financial Intelligence Unit-
India, 6th Floor, Hotel Samrat,
Chanakyapuri, New-Delhi - 110021**

There are altogether five reporting formats prescribed for a banking company viz.

- i) Manual reporting of cash transactions
- ii) Manual reporting of suspicious transactions
- iii) Consolidated reporting of cash transactions by Principal Officer of the bank
- iv) Electronic data structure for cash transaction reporting
- v) Electronic data structure for suspicious transaction reporting.

The RE shall adopt the format prescribed for banks with suitable modifications. NBFCs were also advised to initiate urgent steps to ensure electronic filing of cash transaction report (CTR) as early as possible. The related hardware and technical requirement for preparing reports in an electronic format, the related data files and data structures thereof were furnished in the instructions part of the concerned formats. The RE shall adhere to the following:

- (a) The cash transaction report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. While filing CTR, individual transactions below rupees fifty thousand may not be included. Cash transaction reporting by branches/offices of the RE to their Principal Officer shall invariably be submitted on monthly basis (not on fortnightly basis) and the Principal Officer, in turn, should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.
- (b) The Suspicious Transaction Report (STR) shall be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report shall be made available to the competent authorities on request.
- (c) The Principal Officer shall be responsible for timely submission of CTR and STR to FIU-IND.
- (d) Utmost confidentiality shall be maintained in filing of CTR and STR with FIU-IND. The reports may be transmitted by speed/ registered post, fax, email at the notified address
- (e) The reports for all the branches shall be filed in one mode i.e. electronic or manual;
- (f) A summary of cash transaction report for the RE as a whole may be compiled by the Principal Officer of the RE in physical form as per the format specified. The summary shall be signed by the Principal Officer and submitted both for manual and electronic reporting.
- (g) The RE shall not put any restrictions on operations in the accounts where an STR has been made. However, it shall be ensured that there is no tipping off to the customer at any level. It is likely that in some cases, transactions are abandoned/ aborted by customers on being asked to give some details or to provide documents. The RE shall report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction
- (h) No nil reporting shall be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

17. Procedure For Freezing Of Funds, Financial Assets Or Economic Resources Or Related Services

WSSBL is aware that Under section 51A of Unlawful Activities (Prevention) Act, 1967, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

18. Procedure For Unfreezing Of Funds, Financial Assets Or Economic Resources Or Related services

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to the concerned stock exchanges/depositories and registered intermediaries.

The stock exchanges/depositories and registered intermediaries shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph 5(ii) above within two 21 working days.

The Joint Secretary (IS-I), MHA, being the nodal officer for (ISI) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned stock exchanges, depositories and registered intermediaries.

However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant

19. Co-Operation with Authorities

- **The Company** and its staff shall cooperate with Anti Money Laundering authorities and shall comply with requirements for reporting any suspicious transactions/activity. However, due regard must be paid to the Company's policy of maintaining customer confidentiality. Confidential information about customers may, therefore, only be given to the authorities when there is a legal obligation to do so.
- The Company and its staff shall strictly ensure that there is no 'tipping-off' to customers about suspicious transaction report being made about their transactions/activities or that the authorities are looking into their transactions/activities. If such information is passed to a customer, it may seriously hamper the enquiry/investigation of the authorities
- There may be occasions when the authorities ask for a suspect account to be allowed to continue to operate while they progress with their enquiries. In such cases, the Company would cooperate with the authorities, as far as possible, within the bounds of commercial prudence and applicable laws. Senior line management and Principal/Compliance Officer must always be kept aware of such instances.

20. Implementation of Aadhaar:

As per notification given by the MINISTRY OF FINANCE (Department of Revenue) on 1st June,2017 under Prevention of Money-laundering (Maintenance of Records) Second Amendment Rules, 2017.

The Aadhaar has become mandatory and we have a policy to collect Aadhaar number along with supporting documents from all the clients.

Definitions:

- "Aadhaar number" means an identification number as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
- "Authentication" means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act,2016;
- "Resident" means an individual as defined under sub-section (v) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
- "Identity information" means the information as defined in sub-section (n) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;
- "e - KYC authentication facility" means an authentication facility as defined in Aadhaar (Authentication) Regulations, 2016;
- "Yes/No authentication facility" means an authentication facility as defined in Aadhaar (Authentication) Regulations, 2016;

We are complying with important requirements as mentioned in the notification are emphasize as under:

In these there are two types of clients:

- Individual
- Other than Individual i.e. Entities

In case of Individual:

- The client shall submit to us the Aadhaar number issued by the Unique Identification Authority of India.

In case of other than Individual i.e. Entities:

- Client is a Company/Partnership firm/Trust/ Unincorporated association or body of individuals, shall submit to us certified copies of **Aadhaar Numbers**; Issued to managers, officers or employees in case of company and the person in case of partnership firm/trust/unincorporated association or a body of individuals holding an attorney to transact on behalf of the client entity.
- At the time of receipt of the Aadhaar number under provisions of this rule, shall carry out authentication using either e-KYC authentication facility or Yes/No authentication facility provided by Unique Identification Authority of India (UID).
- If the client does not submit the Aadhaar number, at the time of commencement of an account based relationship with Wellworth Financial Services Private Ltd., then they submit the same within a period of six months from the date of the commencement of the account based relationship.
- For existing clients already having an account based relationship with reporting entities prior to date of this notification i.e. June 1, 2017, the client shall submit the Aadhaar number by December 31, 2017.
- If client fails to submit the Aadhaar number within the aforesaid time limits the said account shall cease to be operational till the time Aadhaar number is submitted by the client.
- In case the identity information relating to the Aadhaar number submitted by the client does not have current address of the client, the client shall submit an officially valid document to the Wellworth Financial Services Private Ltd.

In view of the Supreme Court judgement dated 26.09.2018 regarding Aadhaar Card not being mandatory for registration of clients in the Capital Market, the provision of the above point is not applicable and hence the above point is no longer valid

21. Hiring of Employees:

The RE shall have a sufficient system of screening the employees before their appointment so that they are suitable and competent to perform their duties. The RE shall also provide training programme to its employees on periodic basis, which adequately train them in AML and CFT procedures.

22. Employee Training

- The RE shall have an ongoing employee training programme so that the members of staff are adequately trained in AML/CFT policy. The focus of the training shall be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff needs to be specially trained to handle issues arising from lack of customer education. Proper staffing of the audit function with persons adequately trained and well-versed in AML/CFT policies of the bank, regulation and related issues should be ensured.
- All new staff including temporary or contract staff who may be involved in customer business shall receive suitable and timely induction training to ensure that they understand the RE's approach to money laundering deterrence, including:

- i. What money laundering is?
 - ii. The Company's requirements under the Policy, Company Policies & Procedures and additional policy and standards issued under the Company's Money Laundering Deterrence Programme, as appropriate.
 - iii. Legal or regulatory requirements and the risk of sanctions for themselves, the Company.
 - iv. Reporting requirements as prescribed by SEBI.
 - v. The role played by their Principal / Compliance Officer in money laundering deterrence.
 - vi. The need to protect the Company's reputation.
 - vii. The company should also carry out Investors' Education by preparation of AML and CFT specific literature/ pamphlets which would be forming a part of the KYC or will be separately give to the clients for their educate about PMLA.
- Staff in high-risk areas should receive appropriate training to enable them to understand the money laundering techniques which are likely to be used in their area, and to remind them of their personal responsibilities under the Policy, Company Policies & Procedures other applicable Company Policy and standards and local legal requirements.

23. Further Information

Any queries or doubts concerning Company AML Policy & Procedures or any local legislation or regulation or Circulars or Guidelines relating to Anti Money Laundering and/or Combating Financing of Terrorism shall be referred to the Principal Officer of the Company.

24. Review

- a. The policy shall be reviewed periodically and shall be updated as per the directions/ Circulars issued by RBI and other regulatory authorities from time to time.
- b. The company has made the PMLA policy which is informed to the Investors through the company's website and the company is also carrying out Investor Education initiative by explaining the investors about the PMLA rules & requirements.